

## Circuit arrangement for safety-critical control systems

**Patent number:** DE4341082

**Publication date:** 1995-06-08

**Inventor:** GIERS BERNHARD (DE)

**Applicant:** TEVES GMBH ALFRED (DE)

**Classification:**

- **international:** B60T8/88; G05B19/042; B60T8/88; G05B19/04; (IPC1-7): G06F11/18; G05B9/03; B60K28/16; B60T8/88

- **europen:** B60T8/88B; G05B19/042S

**Application number:** DE19934341082 19931202

**Priority number(s):** DE19934341082 19931202

**Also published as:**

WO9515518 (A1)

EP0731937 (A1)

US5862502 (A1)

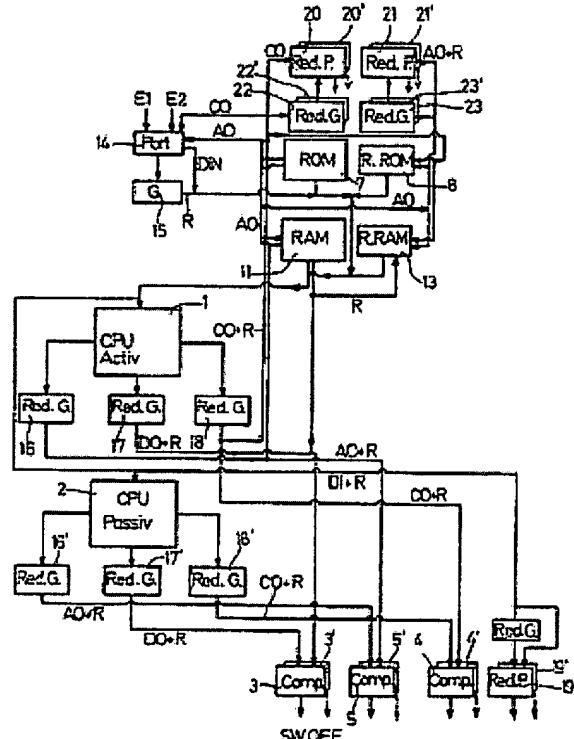
EP0731937 (B1)

[Report a data error here](#)

Abstract not available for DE4341082

Abstract of corresponding document: **US5862502**

PCT No. PCT/EP94/03623 Sec. 371 Date May 31, 1996 Sec. 102(e) Date May 31, 1996 PCT Filed Nov. 4, 1994 PCT Pub. No. WO95/15518 PCT Pub. Date Jun. 8, 1995A circuit arrangement for safety-critical control systems, for example, for the control of anti-lock brake systems, is based on an at least partly redundant processing of input data which are taken into account for generating control signals. The control system is disconnected upon non-correlation of the signals. A microprocessor system is provided for data processing and includes two or more central processor units permitting parallel processing of the input data. The output data of the CPUs are checked for correlation. Each write/read memory of the microprocessor system has a generator to generate a test information. The write/read memories and the read-only memories are extended by memory spaces for the test information. In every writing or reading access to the memories, the contents of the memory space is tested with the associated test information for correlation, and an error identification signal is generated in the absence of correlation or plausibility.





⑯ Aktenzeichen: P 43 41 082.0

⑯ Anmeldetag: 2. 12. 93

⑯ Offenlegungstag: 8. 6. 95

## ⑯ Anmelder:

ITT Automotive Europe GmbH, 60488 Frankfurt, DE

## ⑯ Erfinder:

Giers, Bernhard, 64380 Roßdorf, DE

⑯ Für die Beurteilung der Patentfähigkeit  
in Betracht zu ziehende Druckschriften:

DE 32 34 637 C2  
 DE 30 24 370 C2  
 DE 42 12 337 A1  
 DE 41 37 124 A1  
 DE 41 37 124 A1  
 DE 41 22 016 A1  
 DE 41 17 099 A1  
 DE 41 01 598 A1

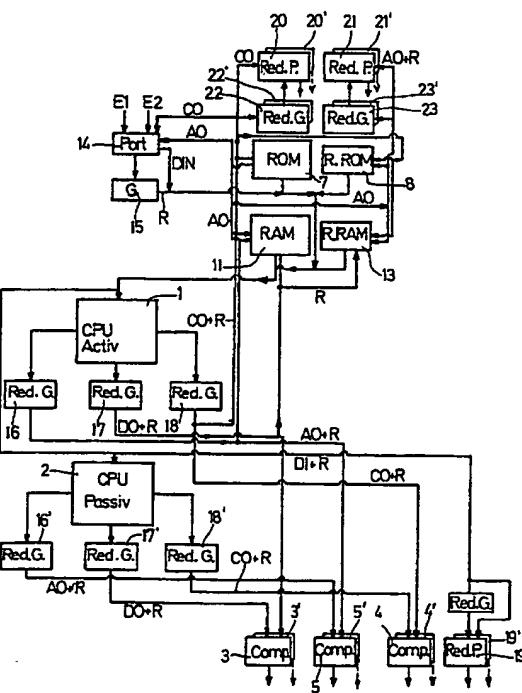
WOBIG, Karl-Heinz: Vom Sinn (und Unsinn) der Di-  
versität bei sicheren Steuerungen. In: ZEV-Glas.  
Ann. 110, 1986, Nr. 12, S. 417-422;  
NIX, Heinz Gerhard: Weniger Ausfälle und hohe Si-  
cherheit durch redundante

Automatisierungssysteme. In: Siemens Energie &  
Automation 8, 1986, H.1, S.2-4;  
NIX, H.G.: Sichere Steuerungen in Mikroprozessor-  
technik. In: messen +  
prüfen/automatik, Juli/August 1984, S.368-370;  
KLING, Uwe;  
SCHRODI, Ewald: Redundantes, hochverfüg-bares  
Automatisierungssystem AS220H im  
dezentralen Prozeßleitsystem Teleperm M. In:  
Siemens-Energie-technik 5, 1983, H.2, S.73-76;  
NIKOLAIZIK, Jürgen;  
u.a.: Fehlertolerante Mikro-computersysteme,  
Verlag Technik GmbH Berlin, 1990, S.68-77;  
JOHNSON, Barry W.: Design and Analysis of  
Fault-Tolerant Digital Systems, Addison-Wesley  
Publishing Company, 1989, S.81-92, S.315-319;  
Patents Abstracts of Japan:  
JP 4- 77901 A., P-1377, June 29, 1992, Vol.16, No.292;  
JP 3-201101 A., P-1281, Nov. 27, 1991, Vol.15, No.469;

## ⑯ Schaltungsanordnung für sicherheitskritische Regelungssysteme

⑯ Eine Schaltungsanordnung für sicherheitskritische Regelungssysteme, z. B. für die Regelung blockiergeschützter Bremsanlagen, beruht auf zumindest teilweise redundant ausgelegter Verarbeitung der Eingangsdaten, die zur Erzeugung der Regelsignale herangezogen werden. Bei Nicht-übereinstimmung der Signale wird das Regelungssystem abgeschaltet.

Zu der Datenverarbeitung ist ein Mikroprozessorsystem vorgesehen, das zwei oder mehrere Zentraleinheiten CPUs (1, 2) enthält, mit denen die Eingangsdaten parallel verarbeitet werden. Die Ausgangsdaten der CPUs werden auf Übereinstimmung überprüft. Den Schreib-/Lesespeichern (11) des Mikroprozessorsystems ist jeweils ein Generator (12) zur Erzeugung einer Prüfinformation zugeordnet. Die Schreib-/Lese- (11) sowie die Festwertspeicher (7) sind durch Speicherplätze (8, 13) für die Prüfinformation erweitert. Bei jedem schreibenden oder lesenden Zugriff zu den Speichern wird der Inhalt des Speicherplatzes (8, 13) mit der zugehörigen Prüfinformation korreliert und ein Fehlererkennungssignal erzeugt, wenn keine Übereinstimmung bzw. "Plausibilität" besteht.



BEST AVAILABLE COPY

## Beschreibung

Die Erfindung bezieht sich auf eine für sicherheitskritische Regelungssysteme vorgesehene Schaltungsanordnung, mit der durch Datenverarbeitung, die zumindest teilweise redundant ausgelegt ist, Eingangssignale ausgewertet und Regelsignale erzeugt werden, wobei zur Ermittlung von Fehlern Ergebnisse der redundanten Datenverarbeitung verglichen und bei Nicht-Übereinstimmung Signale zur Fehlererkennung bzw. Abschaltung oder Sperrung des Regelungssystems gewonnen werden.

Ein Beispiel einer solchen Schaltungsanordnung, die zur Steuerung und Überwachung einer blockierschützten Fahrzeugbremsanlage dient, ist aus der Patentschrift DE 32 34 637 C2 bekannt. Nach dieser Schrift werden die Eingangsdaten zwei identisch programmier-ten Mikrocomputern parallel zugeführt und dort synchron verarbeitet. Die Ausgangssignale (und Zwischen-signale) der beiden Mikrocomputer werden auf Übereinstimmung überprüft. Wenn die Signale voneinander abweichen, wird ein Abschaltsignal ausgegeben. Bei dieser bekannten Schaltung dient einer der beiden Mikrocomputer zur Erzeugung der Bremsdrucksteuersteuer-signale, der andere lediglich zur Bildung der Prüfsignale. Nach diesem Konzept ist eigens zum Zweck der Erkennung eines Datenverarbeitungsfehlers ein zweiter Mikrocomputer, der in seinem Aufbau und seiner Programmierung mit dem ersten Mikrocomputer identisch ist, vorgesehen.

Nach einer anderen bekannten, in der Offenlegungsschrift DE 41 37 124 A1 beschriebenen Schaltungsanordnung werden die Eingangsdaten ebenfalls zwei Mikrocomputern zugeführt, von denen jedoch nur einer die vollständige, aufwendige Signalverarbeitung aus-führt. Der zweite Microcomputer dient vornehmlich zur Überwachung, weshalb die Eingangssignale nach Aufbereitung und Bildung von zeitlichen Ableitungen mit Hilfe vereinfachter Regelalgorithmen und vereinfachter Regelphilosophie weiter verarbeitet werden. Die ver-einfachte Verarbeitung reicht zur Erzeugung von Signa- len aus, die durch Vergleich mit den in dem aufwendigeren Mikrocomputer verarbeiteten Signale Rückschlüsse auf den ordnungsgemäßen Betrieb zulassen. Durch die- se Verwendung eines Prüf-Mikrocomputers geringerer Leistungsfähigkeit lässt sich zwar der Herstellungsauf-wand im Vergleich zu einem System mit zwei Mikro-computern gleicher Leistung reduzieren, doch ist immer noch der für die Fehlererkennung erforderliche Auf-wand erheblich.

Der Erfindung liegt daher die Aufgabe zugrunde, eine Schaltungsanordnung der eingangs genannten Art zu entwickeln, die sich gegenüber den vorgenannten be-kannten Schaltungen durch verringerten Herstellungs-aufwand auszeichnet und die dennoch mit "hoher Si-cherheit Fehler in der Datenverarbeitung erkennt und signalisiert.

Es hat sich gezeigt, daß diese Aufgabe durch eine Schaltungsanordnung gelöst werden kann, deren Besonderheit darin besteht, zur Datenverarbeitung ein Mikroprozessorsystem vorgesehen ist, das zwei oder meh-rere Zentraleinheiten (CPU's) enthält, in denen die Ein-gangssdaten parallel verarbeitet werden, daß Ausgangsdaten einer CPU, nämlich zumindest die Rechenergebnisse (Datenverarbeitungs-Ergebnisse) bzw. "Daten" oder diese Daten, die Adressen und/oder die Ablaufsteuerungsdaten, mit den entsprechenden Ausgangsdaten der zweiten bzw. anderen CPU's vergli-

chen werden und bei Nicht-Übereinstimmung ein Fehlererkennungssignal erzeugt wird, daß den Schreib-/Lesespeichern des Mikroprozessorsystems jeweils ein Generator zur Erzeugung einer Prüf-information zugeordnet und die Schreib-/Lesespeicher sowie die Festwertspeicher durch Speicherplätze für die Prüfinformation erweitert sind, und daß bei jedem schreibenden oder lesenden Zugriff zu den Speichern der Inhalt des Speicherplatzes mit der zugehörigen Prüfinformation verglichen bzw. korreliert und ein Fehlererkennungssignal erzeugt wird, wenn Übereinstimmung oder "Plausibilität" nicht gegeben ist.

Erfindungsgemäß wird die geforderte hohe Sicherheit der Erkennung von Datenverarbeitungsfehlern 15 trotz Verzicht auf einen zweiten, die Eingangssignale redundant verarbeitenden Mikrocomputer erreicht. Es genügt ein einziger Mikrocomputer, der sich von her-kömmlichen Schaltkreisen dieser Art im wesentlichen nur durch redundante Verarbeitung der Eingangsdaten 20 mit Hilfe zweier CPU's und durch relativ geringfügige Erweiterung der Speicher durch Speicherplätze für Prüfinformationen, durch zusätzliche, z. B. aus einigen Exklusiv-ODER-Gattern bestehende Generatoren zur Erzeugung der Prüf- oder Redundanzinformation und 25 durch einige zusätzliche Vergleicher unterscheidet.

Die Erweiterung der Speicher durch Plätze für die Prüf- bzw. Redundanzinformationen beschränkt sich — je nach geforderter Redundanz — auf einige Prozent, z. B. 5 bis 20%, des für den Speicher erforderlichen Platzes. Die Verwendung von zwei vollständigen CPU's fällt 30 im Vergleich zu dem Aufwand für das gesamte Mikroprozessorsystem nur wenig ins Gewicht. Der Herstel-lungsaufwand für das erfundungsgemäße Mikroprozes-sorsystem, das vorzugsweise auf einem Chip unterge-35 bracht wird, ist folglich nur wenig höher als für ein ver-gleichbares Chip bekannter Art. Die Beschränkung auf nur ein Mikroprozessorsystem im Vergleich zu entspre-chenden Schaltungen bekannter Art, die zwei Prozessoren besitzen, führt also zu erheblichen Einsparungen.

Einige vorteilhafte Ausführungsarten der erfundungs-gemäßen Schaltungsanordnung sind in den Unteran-sprüchen beschrieben.

Ein Ausführungsbeispiel der Erfindung besteht darin, daß die Prüfinformation in Form von Redundanzinfor-mation vorliegt. Zweckmäßig ist es, zur Bildung der Prüf- bzw. Redundanzinformation die gerade oder un-gerade Parität der Bits der einzelnen Daten zu ermit-teln. Es kann jedoch auch die Quersumme der gespei-cherten oder übertragenen Daten oder einer Redundan-zinformation auf Basis eines vorgegebenen Polynoms 40 gebildet werden.

Nach einer weiteren vorteilhaften Ausführungsart der Erfindung werden zur Erzeugung der Prüf- bzw. Redundanzinformation die gespeicherten und/oder die 45 übertragenen Daten durch ein Paritätsbit erweitert. Der zusätzliche Speicherplatzbedarf für dieses Prüfbits fällt kaum ins Gewicht.

Das Fehlererkennungssignal führt nach einem weite- 50 ren Ausführungsbeispiel der Erfindung zur Abschaltung oder zur Sperrung des Mikroprozessorsystems. Bei Verwendung der erfundungsgemäßen Schaltungsanord-nung zur Blockierschutzregelung wird durch Abschal-tung des Mikroprozessorsystems die Regelung beendet und die konventionelle Bremsenfunktion, d. h. die Brem-senfunktion ohne Regelung, sichergestellt.

Eine Weiterbildung der erfundungsgemäßen Schal-tungsanordnung besteht darin, daß zur Erhöhung der Redundanz nicht nur die CPU's, sondern noch weitere



ausgewählte Komponenten des Mikroprozessorsystems, wie Speicher, Eingabe-Ausgabe-Einheiten usw., zweifach in diesem 1-Chip-Mikroprozessorsystem vorhanden sind.

Ein sicherheitskritisches Regelungssystem, für das sich die erfindungsgemäße Schaltungsanordnung besonders eignet, ist eine Kraftfahrzeug-Bremsanlage mit Blockierschutz- und/oder Antriebsschlupfregelung. In diesem Fall werden die Sensorsignale, die das Drehverhalten der Räder und/oder das Fahrverhalten des Fahrzeugs wiedergeben, mit dieser Schaltungsanordnung verarbeitet und zur Erzeugung von Bremsdruck-Steuerignalen ausgewertet.

Weitere Merkmale, Vorteile und Anwendungsmöglichkeiten der Erfahrung gehen aus der folgenden Beschreibung spezieller Ausführungsbeispiele anhand der beigefügten Abbildungen hervor.

Es zeigen in Prinzipdarstellung als Blockschaltbild und in Teildarstellung

Fig. 1 das Zusammenwirken der Zentraleinheiten (CPU's), der zugehörigen Vergleicher und der Abschaltfunktion eines Mikroprozessorsystems nach der Erfahrung.

Fig. 2 in gleicher Darstellungsweise wie Fig. 1 einen Festwertspeicher (ROM) und die zugehörigen Prüf-Komponenten,

Fig. 3 in gleicher Darstellungsweise wie Fig. 2 einen Schreib-/Lesespeicher und die zugehörigen Prüf-Komponenten,

Fig. 4 in gleicher Darstellungsweise den Anschluß von Eingabe- oder Ausgabeeinheiten und

Fig. 5 in gleicher Darstellungsweise wie die vorangegangenen Figuren die Zusammenschaltung der wesentlichen Komponenten eines Mikroprozessorsystems nach der Erfahrung.

Fig. 1 veranschaulicht, daß das erfindungsgemäße Mikroprozessorsystem zwei Zentraleinheiten 1, 2, CPU's genannt, aufweist, denen über Bus-Systeme, nämlich einen Datenbus DATA IN, einen Steuerbus CONTROL DATA IN und einen Adreßbus ADDRESS IN die Eingangssignale bzw. Eingangsdaten parallel zugeführt werden. Die CPU 1 wird als "aktiv" bezeichnet, weil ihre Ausgangsdaten über die Bus-Systeme D OUT, C OUT, A OUT zur Weiterverarbeitung weitergeleitet werden. Die CPU 2 ist dagegen "passiv", weil sie lediglich zu Prüfzwecken vorhanden ist. Da beide CPU's 1, 2 in dem vorliegenden Beispiel identisch aufgebaut und programmiert sind, lassen sich durch Vergleich der Ausgangsdaten beider Einheiten 1, 2 Datenverarbeitungsfehler erkennen. Die Ausgangsdaten der beiden CPU's werden daher mit Hilfe von Vergleichern 3, 4, 5 auf Übereinstimmung verglichen; dem Datenbus, dem Steuerbus und dem Adreßbus sind jeweils ein eigener Vergleicher 3 bzw. 4 und 5 zugeordnet. Stimmen die Daten nicht überein, wird dies als Datenverarbeitungsfehler bewertet und über ein Gatter 6 ein Abschalt- oder Sperrsignal ausgegeben.

In Bezug auf die Datenverarbeitung in den CPU's 1, 2 ist also bei dem erfindungsgemäßen Mikroprozessorsystem 100%ige Redundanz gegeben. Die Prüfung und Überwachung der Speicher beruht auf einem anderen Prinzip. Wie Fig. 2 zeigt, ist einem Festwertspeicher (ROM) 7 ein weiterer Speicher 8 für Redundanzinformationen zugeordnet. In der Praxis wird der Festwertspeicher 7 zur Aufnahme dieser Redundanzinformationen um die entsprechenden Speicherplätze erweitert.

Die aus dem Speicher 7 ausgelesenen Daten werden einem Prüf- oder Redundanz-Generator 9 zugeführt,

der Logikschaltungen zur Erzeugung der Prüf-Informationen enthält. Die mit Hilfe des Generators 9 gewonnenen Prüfinformationen müssen mit den im Speicher 8 enthaltenen Informationen übereinstimmen. Trifft dies nicht zu, wird von einem Vergleicher 10 ein Abschalt- oder Sperrsignal erzeugt.

Liegt die Prüfinformation in Form eines Paritätsbits vor, besteht der Generator 9 zur Bildung dieser Prüf- bzw. Redundanzinformation z. B. aus der erforderlichen Anzahl von Exklusiv-ODER-Gattern zur Feststellung der Parität. Auf diese Weise kann jeder Einfach-Fehler erkannt werden; natürlich lassen sich durch Prüf-Informationen auf Basis von zwei oder mehreren Bits auch gleichzeitige Mehrfachfehler erkennen. Die Bildung von Redundanz-Information auf Basis von Polynomen und bestimmten Algorithmen kann ebenfalls zweckmäßig sein.

Für das Lesen von Informationen aus einem Schreib-/Lesespeicher (RAM) gelten die Erläuterungen anhand der Fig. 2 analog. Auch dieser Schreib-/Lesespeicher wird erfindungsgemäß durch einige Speicherplätze für die Redundanz-Informationen erweitert.

Bei einem schreibenden Zugriff zu einem Schreib-/Lesespeicher 11, siehe Fig. 3, wird mit einem Generator 12, der dem Generator 9 nach Fig. 2 entspricht, eine Prüfinformation erzeugt und in einem Zusatzspeicher 13 – oder zusätzlichen Speicherplätzen im zugehörigen Schreib-/Lesespeicher – abgelegt. Beim lesenden Zugriff auf diese Information wird dann wiederum die Übereinstimmung oder "Plausibilität" überprüft.

Wie Fig. 4 zu entnehmen ist, werden die über eine Eingabeeinheit 14 dem erfindungsgemäßen Mikroprozessorsystem zugeführten Daten analog der bereits erläuterten Behandlungsweise überprüft. Es werden in einem Generator 15 Prüf- bzw. Redundanzinformationen gebildet. Bei Übertragung oder Weiterverarbeitung der Daten erfolgt dann jeweils die Überprüfung in der beschriebenen Weise.

Die Eingabeeinheit 14 erhält die zu verarbeitenden Eingangssignale über doppelt ausgelegte Wege – symbolisiert durch die beiden Eingangspfeile E1, E2 in Fig. 4 – aus der zugehörigen Quelle. Die Prüfrendanz kommt erst nach Erfassung der Signale durch das erfindungsgemäße Mikroprozessorsystem zum Tragen.

Grundsätzlich wird die Anzahl der durch die Redundanzgeneratoren generierten Informationen durch die jeweiligen Forderungen nach Erkennung von Einfach- oder Mehrfachfehlern festgelegt. Ist für einen Anwendungsfall die Erkennung von Einfachfehlern ausreichend, wird der Redundanzgenerator (9, 15) am einfachsten durch eine Kette von Exklusiv-ODER-Gattern verwirklicht. Sollen auch Doppelfehler erkennbar sein, so werden mehrere Redundanzbits, z. B. durch Bilden der Quersumme bzw. Addieren aller Bits eines Wortes, gebildet. Die "Größe" der Prüfinformationen läßt sich somit in Abhängigkeit von der geforderten Sicherheit gegen gleichzeitige auftretende Fehler variieren.

Die anhand der Fig. 1 beschriebenen Vergleicher 3, 4, 5 lassen sich z. B. durch Komparatorschaltungen realisieren, die "bit"-weise alle Informationen vergleichen. Eine mögliche Ausführungsform ist der bit-weise Vergleich durch die vorgenannten Exklusiv-ODER-Gatter, deren Ausgänge durch ein weiteres ODER-Gatter zusammengefaßt werden.

Der Vergleicher 10 nach Fig. 2 vergleicht die aus dem Speicher 7 ausgelesene Information, die durch die in dem Redundanzgenerator 9 erzeugte Redundanzinformation erweitert ist, mit der Prüf-Information aus dem



Speicher 8. Diese Überprüfung geschieht wiederum z. B. mit Hilfe der zuvor genannten Exklusiv-ODER-Gatter.

Die Sicherheit der Fehlererkennung mit Hilfe der erfundungsgemäßen Schaltungsanordnung lässt sich bei Bedarf noch durch folgende Maßnahmen erhöhen: Die Vergleicher und/oder Abschaltfäden können mehrfach ausgelegt werden. Ein "schlafender" Fehler innerhalb eines Vergleichers oder eines Abschaltfadens kann dann eine Systemabschaltung im Fehlerfalle nicht mehr verhindern.

Grundsätzlich ist es auch möglich, einen Vergleicher außerhalb des eigentlichen Mikroprozessorschips anzutragen. Da ein externer Vergleicher zyklisch Werte aus dem Chip erhält, kann der Vergleicher durch eine zweite Taktversorgung das Zeitverhalten der CPU's überprüfen und im Fehlerfall eine Abschaltung des Regelungssystems hervorrufen. Als Überprüfungskriterien dienen sowohl der Dateninhalt der empfangenen Informationen als auch das zeitliche Verhalten der Signale.

Zur Reduzierung der Übertragungsbandbreite zwischen Vergleicher und den CPU's kann eine zusätzliche Logik verwendet werden, die bestimmte Informationen auswählt und jedes n-te Resultat zum externen Vergleicher weiterleitet. Durch ein derartiges Auswahlssystem kann die Anzahl der überprüften Stichproben auf ein noch geringeres, noch ausreichendes Maß reduziert werden.

Des weiteren ist es grundsätzlich möglich, lediglich die empfangene Prüf- bzw. Redundanzinformation und die zum Vergleich berechnete Information durch einen externen Schaltkreis zu überprüfen. Die Anzahl der zu dem externen Schaltkreis zu übermittelnden Signale lässt sich auf diese Weise reduzieren.

Fig. 5 dient zur Veranschaulichung des Zusammenwirkens der einzelnen bereits beschriebenen oder diskutierten Komponenten eines Mikroprozessorsystems nach der Erforschung. Soweit Übereinstimmung mit den Ausführungsbeispielen nach den Fig. 1 bis 4 besteht, wurden gleiche Bezeichnungen in Fig. 5 verwendet.

Die Ausgangsdaten der Zentraleinheiten 1, 2 sind in Fig. 5 mit DO (Data OUT), die Adressdaten mit AO (Adress OUT) und die Ablaufsteuerungsdaten mit CO (Control OUT) bezeichnet. "R" deutet auf die zugehörige Prüf- bzw. Redundanzinformation hin. Die Eingangsdaten sind mit "I" (DI, AI, CI) bezeichnet.

Abweichend von dem Ausführungsbeispiel nach Fig. 1 werden die Ausgänge der Zentraleinheiten oder CPU's (1, 2) über Redundanzgeneratoren 16, 17, 18 bzw. 16', 17', 18', die der übertragenen Information eine Prüfinformation, z. B. ein Prüfbit hinzufügen, zu den Vergleichern 3, 4, 5, weitergeleitet. Wie in Fig. 5 angedeutet ist, sind jeweils zwei Vergleicher 3, 3'; 4, 4'; 5, 5' parallelgeschaltet. Jeder Vergleicher ist in der Lage, ein Fehlererkennungs- oder Abschaltignal (Switch OFF) abzugeben. Zur Überprüfung der Eingangsdaten DI + R ("R" symbolisiert die Prüf- bzw. Redundanzinformation) ist eine weitere Schaltungskomponente 19, 19' vorhanden, die ebenfalls ein Abschaltignal SW OFF erzeugt, wenn die Information und das zugehörige Prüfsignal nicht plausibel sind.

Abweichend von Fig. 1 sind der besseren Übersicht wegen in Fig. 5 die Signaleingänge der Zentraleinheit 1, 2 für die Adress- und Steuerdaten nicht dargestellt, sondern lediglich der Dateneingang DI bzw. DI + R.

Die Anschaltung des Schreib-/Lesespeichers RAM 11 mit dem zugehörigen Speicher 13 für die Prüf- bzw. Redundanzinformation sowie des Festwertspeichers (ROM) 7 und des zugehörigen Prüfspeichers 8 wurden

bereits anhand der Fig. 2 und 3 erläutert; es besteht kein Unterschied gegenüber dem Ausführungsbeispiel nach Fig. 5. Die Eingabeeinheit 14 mit dem zugehörigen Redundanzgenerator 15 wurden ebenfalls bereits anhand der Fig. 4 erläutert. Wiederum werden zwei in die Eingangssignale E1, E2 parallel zugeführt.

Zur Überprüfung der Ablaufsteuerungsdaten (Controldaten) und der Adressdaten sind die Schaltungskomponenten 20, 20' und 21, 21' vorgesehen, die ebenfalls jeweils zweifach vorhanden sind. Wird in diesen Schaltungskomponenten eine Nicht-Übereinstimmung oder fehlende Plausibilität zwischen den Daten und den zugehörigen Prüfinformationen festgestellt, wird wiederum ein Abschaltignal SW OFF erzeugt. Die zugehörigen Redundanzgeneratoren sind mit 22, 22' und 23, 23' bezeichnet.

### Patentansprüche

1. Schaltungsanordnung für sicherheitskritische Regelungs-Systeme, mit der durch Datenverarbeitung, die zumindest teilweise redundant ausgelegt ist, Eingangssignale ausgewertet und Regelsignale erzeugt werden, wobei Ergebnisse der redundanten Datenverarbeitung verglichen und bei Nicht-Übereinstimmung Signale zur Fehlererkennung bzw. Abschaltung oder Sperrung des Regelungssystems gewonnen werden, dadurch gekennzeichnet,

daß zur Datenverarbeitung ein Mikroprozessorsystem vorgesehen ist, das zwei oder mehrere Zentraleinheiten bzw. CPU's (1, 2) enthält, in denen die Eingangsdaten (DI, AI, CI) parallel verarbeitet werden, daß Ausgangsdaten einer CPU, nämlich zumindest die Rechenergebnisse (Datenverarbeitungs-Ergebnisse) bzw. "Daten", mit den entsprechenden Ausgangsdaten der zweiten bzw. der anderen CPU's verglichen werden und bei Nicht-Übereinstimmung ein Fehlererkennungssignal (SW OFF) erzeugt wird,

daß den Schreib-/Lesespeichern (11) des Mikroprozessorsystems jeweils ein Generator (12) zur Erzeugung einer Prüfinformation zugeordnet ist und die Schreib-/Lesespeicher (11) sowie die Festwertspeicher (7) (7) durch Speicherplätze (13, 8) für die Prüfinformation erweitert sind, und

daß bei jedem schreibenden oder lesenden Zugriff zu den Speichern (11) der Inhalt des Speicherplatzes mit der zugehörigen Prüfinformation verglichen bzw. korreliert und ein Fehlererkennungssignal (SW OFF) erzeugt wird, wenn Übereinstimmung oder "Plausibilität" nicht gegeben ist.

2. Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß sowohl die Rechenergebnisse bzw. "Daten" als auch die Adressen und/oder die Ablaufsteuerungsdaten mit den entsprechenden Ausgangsdaten der zweiten bzw. der anderen CPU's verglichen werden und bei Nicht-Übereinstimmung das Fehlersignal (SW OFF) erzeugt wird.

3. Schaltungsanordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Prüfinformation in Form von Redundanzinformation (R) vorliegt.

4. Schaltungsanordnung nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß zur Erzeugung der Prüf- bzw. Redundanzinformation (R) die gerade oder ungerade Parität der Bits der einzelnen Daten ermittelt wird.

5. Schaltungsanordnung nach einem oder mehreren



der Ansprüche 1 bis 3, dadurch gekennzeichnet,  
daß zur Erzeugung der Prüfinformation die Quer-  
summen der die einzelnen gespeicherten oder  
übertragenen Daten darstellenden Zahlen oder ei-  
ne Redundanzinformation auf Basis eines vorgege- 5  
benen Polynoms oder Algorithmus gebildet wird.

6. Schaltungsanordnung nach einem oder mehreren  
der Ansprüche 1 bis 5, dadurch gekennzeichnet,  
daß zur Erzeugung der Prüf- bzw. Redundanzinfor- 10  
mation die gespeicherten und/oder die übertrage-  
nen Daten durch ein Paritätsbit erweitert werden.

7. Schaltungsanordnung nach einem oder mehreren  
der Ansprüche 1 bis 6, dadurch gekennzeichnet,  
daß die Eingangsdaten in den CPU's (1, 2) synchron 15  
verarbeitet werden.

8. Schaltungsanordnung nach einem oder mehreren  
der Ansprüche 1 bis 7, dadurch gekennzeichnet,  
daß das Fehlererkennungssignal (SW OFF) zur Ab-  
schaltung oder Sperrung des Mikroprozessorsy- 20  
stems führt.

9. Schaltungsanordnung nach einem oder mehreren  
der Ansprüche 1 bis 8, dadurch gekennzeichnet,  
daß zur weiteren Erhöhung der Sicherheit der Feh-  
lererkennung zusätzlich zu den CPU's (1, 2) noch 25  
weitere Komponenten des Mikroprozessorsy-  
stems, wie Festwertspeicher (7), Schreib-/Lesespei-  
cher, Eingang-/Ausgangkomponenten (14), Bussy-  
steme etc., zweifach oder mehrfach vorhanden sind,  
wobei mit Vergleichern jeweils die Übereinstim- 30  
mung der Informationen oder die Plausibilität  
überprüft wird.

10. Schaltungsanordnung nach einem oder mehre-  
ren der Ansprüche 1 bis 8, dadurch gekennzeichnet,  
daß diese Bestandteil einer Kraftfahrzeug-Brems-  
anlage mit Blockierschutz- und/oder Antriebs- 35  
schlupfregelung ist und zur Verarbeitung von Si-  
gnalen, die das Drehverhalten der Fahrzeugräder  
und/oder das Fahrverhalten des Fahrzeugs wieder-  
geben, und zum Erzeugen von Bremsdrucksteuersi-  
gnalen dient. 40

Hierzu 3 Seite(n) Zeichnungen

45

50

55

60

65

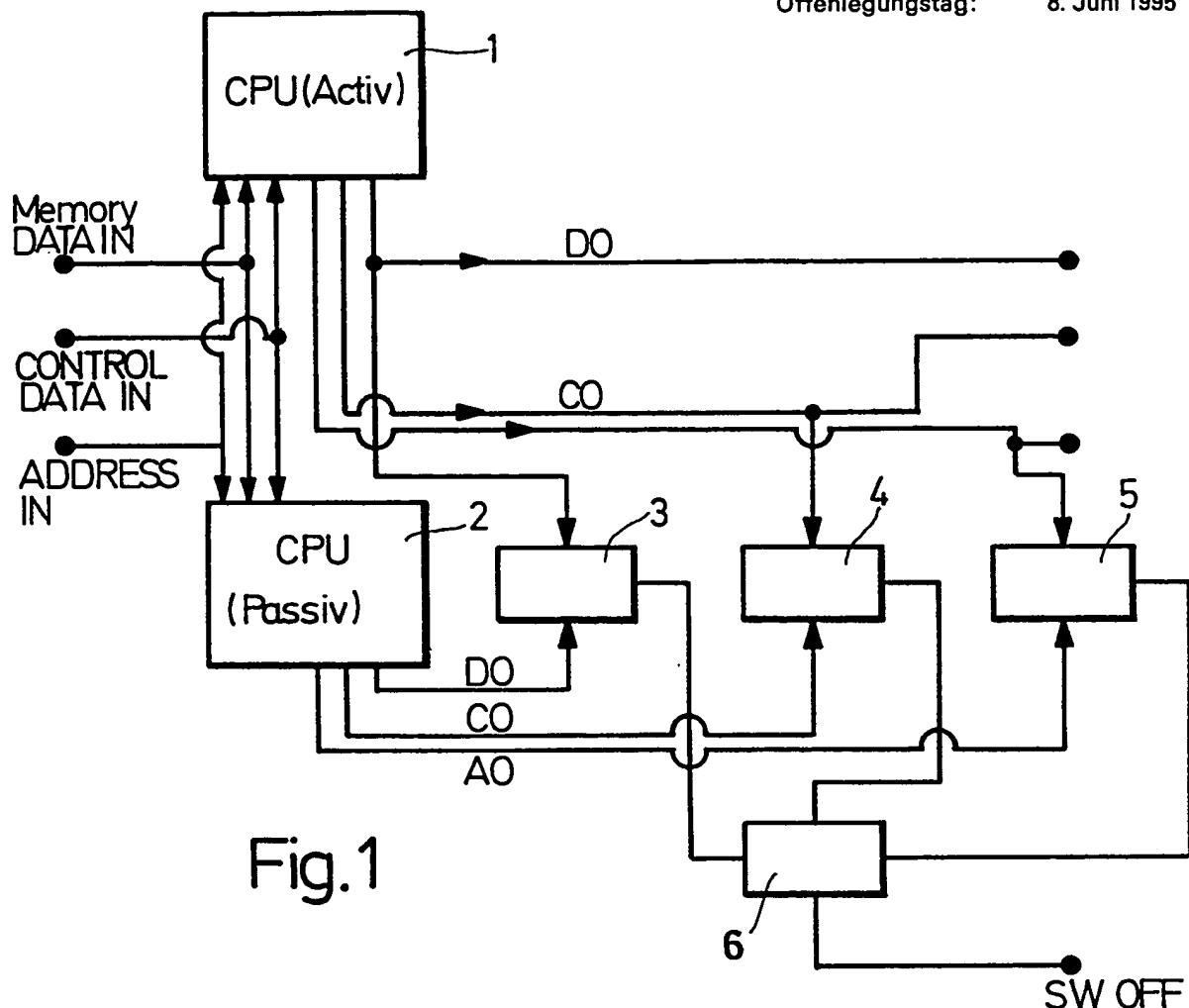


Fig. 1

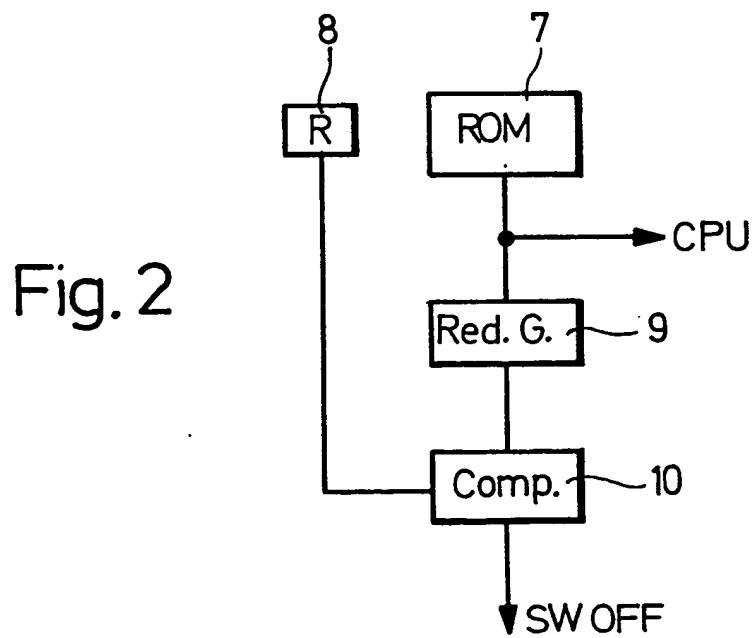
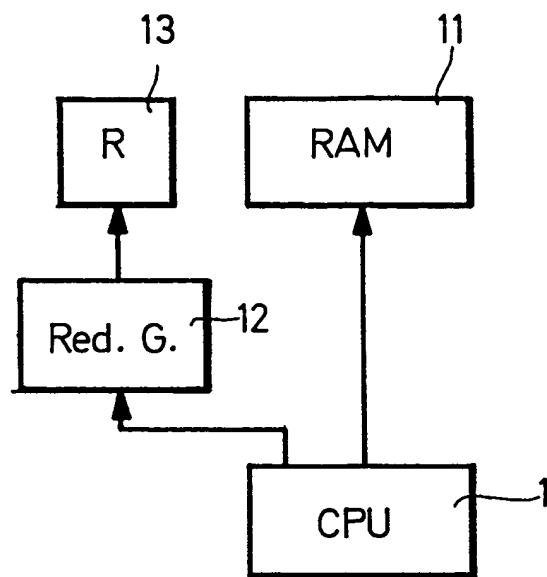
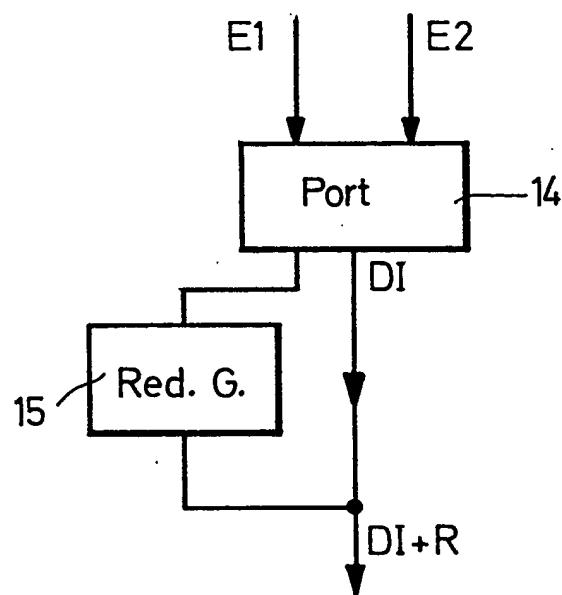


Fig. 2



**Fig. 3**



**Fig. 4**

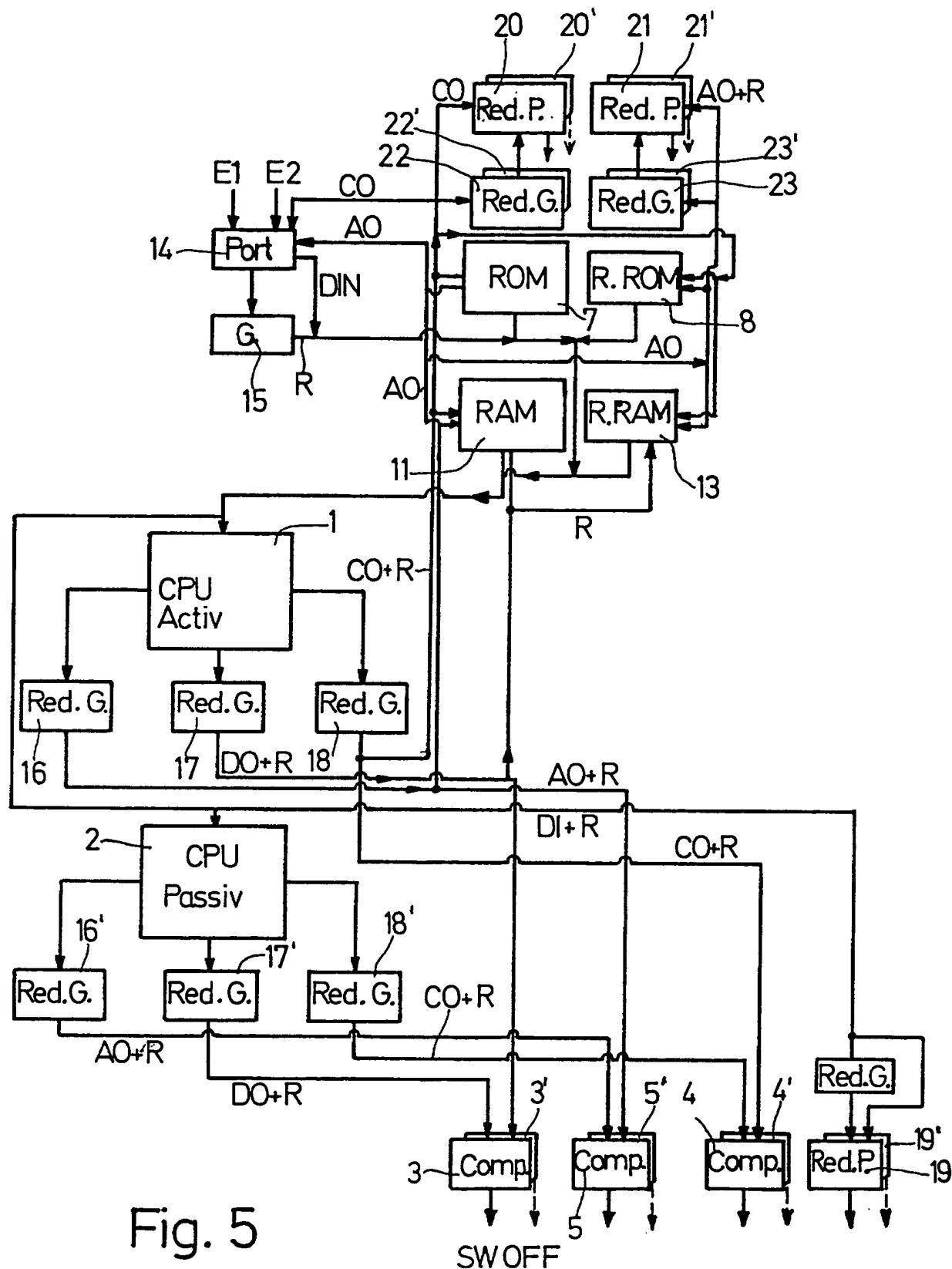


Fig. 5